CLAIM AMENDMENTS

The following is a complete list of claims. The claims below replace all prior versions of the claims in the application. Please amend claims 15 – 25, 27, 28, 30 – 40, 42 – 62, 65 – 68 and 70 – 77. Please add new claims 78 – 82.

1. – 14. Canceled

15. (Currently Amended) A method of protecting media content stored on a ~~creating a protected audio~~ storage medium, the method comprising:

~~storing digital audio data on the audio storage medium;~~

creating a first session on the medium, the first session containing digital ~~audio~~ data stored in ~~according to~~ a first ~~audio data storage~~ format and representing all or substantially all of the media content, the digital data in the first session being readable by an electronic device configured to read digital ~~audio~~ data in ~~stored according to~~ the first ~~audio storage~~ format; ~~:~~

creating a second session on the medium, the second session containing digital data stored in a second format and representing all or substantially all of the media content, the digital data in the second session being readable by a media player associated with a computing device and configured to read the digital data in the second format;

including on the second ~~first~~ session at least one digital rights management license describing allowed uses for the digital ~~audio~~ data;

including on the second ~~first~~ session digital rights management software;

encrypting the digital ~~audio~~ data in ~~on~~ the second ~~first~~ session so that the digital rights management software does not grant access to the digital ~~audio~~ data stored in ~~on~~ the second session ~~audio storage medium~~ unless the digital rights management software determines that a requested access complies with the allowed uses described in the at least one digital rights management license; and

~~creating a second session on the medium, the second session containing audio data stored according to a second audio data storage format, the audio data representing the same audio data contained on the first session and being readable by an audio player associated with a computing device configured to read audio data stored according to the second audio storage format; and~~

preventing the media player associated with the computing device configured to read the digital data in the second format from ~~protecting the audio data contained on the second session so that the electronic device cannot~~ accessing the digital ~~audio~~ data ~~stored~~ in the first format. ~~second session.~~

16. (Currently Amended) The method of claim 15, wherein encrypting the ~~audio~~ data comprises:

separating the media ~~audio~~ content into packets of ~~audio~~ data;

encrypting the packets;

storing the encrypted packets to the medium; and

storing at least one ~~audio~~ decryption key on the medium such that the digital rights management software, when executed by ~~on~~ a computer, causes the computer to use ~~s~~ the at least one decryption key to decrypt the packets. ~~and allows access to the audio.~~

17. (Currently Amended) The method of claim 16, wherein encrypting the ~~audio~~ data further comprises:

creating at least two ~~audio~~ encryption keys;

for every ~~audio~~ encryption key, encrypting at least one packet with that key;

encrypting every packet with the at least two ~~audio~~ encryption keys; and

wherein the at least one ~~audio~~ decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

18. (Currently Amended) The method of claim 17, wherein the ~~audio~~ encryption keys are symmetric, and wherein the method further ~~storing the decryption keys~~ comprises:

generating at least one protection encryption key for each of the at least two ~~audio~~ encryption keys;

encrypting each ~~audio~~ encryption key with an associated protection encryption key;

storing the at least one encrypted ~~audio~~ encryption key on the medium; and ~~, to serve as decryption keys; and~~

storing at least one protection decryption key on the medium, such that the at least one protection decryption key can be used to ~~s~~ decrypt the at least one ~~audio~~ encryption key.

19. (Currently Amended) The method of claim 18, wherein:

the at least one protection encryption key comprises a generic protection decryption key and a unique protection encryption key; and

the at least one protection decryption key ~~s~~ comprises a generic protection decryption key and a unique protection decryption key.

20. (Currently Amended) The method of claim 18, ~~19,~~ wherein storing the at least one protection decryption key ~~s~~ comprises integrating the protection decryption key ~~m~~ inside the digital rights management software.

21. (Currently Amended) The method of claim 15, ~~20,~~ wherein the digital rights management software is ~~made~~ tamper-resistant.

22. (Currently Amended) The method of claim 21, further ~~additionally~~ comprising:

storing ~~placing~~ a binding identifier on the medium, wherein the binding identifier is associated with the at least one digital rights management license, and is used by the digital rights management software to determine whether or not to allow the requested access to the digital data in the second session, and wherein the binding identifier cannot be duplicated onto another storage medium. ~~such that the binding identifier cannot be copied if the contents of the medium are duplicated on another medium;~~

~~associating the at least one digital rights management license with the binding identifier; and~~

~~wherein the digital rights management software does not allow access to the encrypted audio data unless the proper associated unique identifier is present on the medium.~~

23. (Currently Amended) The method of claim 22 wherein:

storing the binding identifier ~~associating the license with the binding identifier~~ comprises encrypting together the at least one license and a copy of the binding identifier that is associated with the at least one license; and ~~together and including this encrypted file on the medium; and~~

~~wherein~~ the digital rights management software compares a decrypted copy of the binding identifier to the binding identifier present on the medium before allowing the requested access. ~~does not allow access to encrypted audio data based on rules described in the encrypted license unless the associated copy of the binding identifier, once decrypted, matches the binding identifier present on the medium.~~

24. (Currently Amended) The method of claim 22, wherein:

storing ~~associating the license with~~ the binding identifier comprises:

creating a license encryption key from ~~using~~ the binding identifier; and ~~as a seed to create a license encryption key; and~~

encrypting the at least one license with the encryption key; and

~~wherein~~ the digital rights management software decrypts the at least one license using a decryption key created from the binding identifier to determine whether or not to allow the requested access to the digital data in the second session. ~~is configured make a determination of whether the software will allow access to the encrypted audio data by using the binding identifier to create a decryption key, and then decrypting the at least one license.~~

25. (Currently Amended) The method of claim 15, wherein:

the digital ~~audio~~ data on the first session comprises a plurality of separate audio recordings;

~~wherein~~ the at least one digital rights management license comprises a plurality of digital rights management licenses; and

~~wherein~~ at least one of the plurality of digital rights management licenses describes allowed uses for a specific recording. ~~track.~~

26. (Original) The method of claim 15, wherein the medium is a compact disc.

27. (Currently Amended) A ~~protected audio~~ compact disc, comprising:

a first session, ~~readable by a n audio~~ compact disc player;

first ~~audio~~ data representing all or substantially all media content on the compact disc, the first data stored on the first session and protected so that the ~~audio~~ first data ~~on the first session~~ cannot be decoded into a renderable media presentation by an optical media drive;

a second session, ~~readable by an optical media drive;~~

second data representing all or substantially all of the media content on the compact disc, the second data stored on the second session and encrypted so that the second data cannot be decoded into a renderable media presentation by the compact disc player;

at least one digital rights management license, written to the second session, and describing allowed uses for the second ~~encrypted digital audio~~ data;

digital rights management software, ~~stored on the second session~~ that, when executed by a computer, causes the computer to use the digital rights management license to determine whether or not a requested use of the second data is allowed, and to prevent the requested use of the second data if the license does not permit the requested use; ~~;~~

~~audio data stored on the second session, the second session audio data representing the same audio contained on the first session, and encrypted so that a computing device executing the digital rights management software will not allow access to the second session audio data unless the computing device determines that the access is in compliance with the allowed uses described in the at least one digital rights management license; and~~

at least one decryption key ~~,~~ stored on the second session and used by ~~,~~ ~~such that~~ the digital rights management software ~~is configured~~ to decrypt the second data. ~~encrypted digital audio data using the decryption key.~~

28. (Currently Amended) The compact disc of claim 27, wherein the encrypted second data ~~audio content~~ comprises a plurality of encrypted packets of ~~audio~~ data.

29. (Original) The compact disc of claim 28, wherein the plurality of encrypted packets are encrypted with a plurality of encryption keys, and wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets.

30. (Currently Amended) The compact disc of claim 27, ~~29,~~ wherein the at least one decryption key is integrated inside the digital rights management software.

31. (Currently Amended) The compact disc of claim 27, ~~30,~~ wherein the digital rights management software is tamper resistant.

32. (Currently Amended) The compact disc of claim 31, further ~~additionally~~ comprising:

a binding identifier ~~,~~ stored on the compact disc, associated with the at least one digital rights management license, and used by the digital rights management software to determine whether or not to allow the requested use of the second data, wherein ~~such that~~ the binding identifier cannot be duplicated onto another compact disc. ~~copied if the contents of the compact disc are duplicated on another compact disc; and~~

~~wherein the at least one digital rights management license is associated with the binding identifier so that the digital rights management software does not allow access to the encrypted audio data unless the proper associated binding identifier is present on the compact disc.~~

33. (Currently Amended) The compact disc of claim 32, further comprising: ~~wherein:~~

the at least one license and a copy of the binding identifier ~~are~~ encrypted together and stored on the second session; and

wherein the digital rights management software, when executed by the computer, also causes the computer to compare a decrypted copy of the binding identifier to the binding identifier present on the disc before allowing a requested use of ~~does not allow access to~~ the second ~~encrypted audio~~ data. ~~based on rules described in the encrypted license unless the associated copy of the binding identifier, once decrypted, matches the binding identifier present on the disc;~~

~~and further comprising a file, stored on the second session on the compact disc, containing encrypted versions of the binding identifier and the at least one digital rights management license.~~

34. (Currently Amended) The compact disc of claim 32, wherein:

the at least one license is encrypted using an encryption key created by using the binding identifier ~~found on the compact disc~~ as a seed; and

the digital rights management software, when executed by the computer, also causes the computer to decrypt the at least one license using a decryption key created from the binding identifier to ~~is configured make a~~ determine ~~ation of~~ whether or not ~~the software is permitted~~ to allow a requested use of the second ~~access to the encrypted audio~~ data. ~~by using the binding identifier to create a decryption key, and then decrypting the at least one license~~

35. (Currently Amended) The compact disc of claim 27, wherein:

the second ~~audio~~ data on the second session comprises a plurality of separate audio recordings;

~~wherein~~ the at least one digital rights management license comprises a plurality of digital rights management licenses; and

~~wherein~~ at least one of the plurality of digital rights management licenses describes allowed uses for a specific audio recording.

36. (Currently Amended) The compact disc of claim 35, wherein the plurality of digital rights management licenses contain ~~s~~ a license describing uses for a

plurality of the audio recordings ~~written on the second session~~ in addition to the at least one license that describes uses for a specific audio recording.

37. (Currently Amended) The compact disc of claim 27, further comprising at least one validation code associated with the digital rights management software ~~and written on the compact disc,~~ wherein the at least one code represents a cryptographically-signed hash of a canonical representation of at least one section of the digital rights management software code, and wherein the digital rights management software, when executed by the computer, causes the computer ~~is configured~~ to detect tampering or replacement of the at least one section of code at the time the code is executed by performing a runtime hash of the at least one section of code and comparing the runtime hash to the stored cryptographically-signed hash.

38. (Currently Amended) The compact disc of claim 27 further comprising protected playback software that, when executed by the computer, causes the computer ~~, written to the compact disc, the playback software configured to be copied to a storage device~~ to play the second ~~audio~~ data.

39. (Currently Amended) A system for protecting media ~~audio~~ content, the system comprising:

a computing device;

~~at least one~~ media ~~audio~~ content ~~file,~~ stored on the computing device;

at least one digital rights management license ~~,~~ stored on the computing device and ~~,~~ describing allowed uses for the ~~at least one~~ media ~~digital audio~~ content; ~~file;~~

digital rights management software ~~,~~ stored on the computing device and that, when executed by the computing device, causes the computing device to use the digital rights management license to determine whether or not a requested use of the second data is allowed, and to prevent the requested use of the second data if the license does not permit the requested use; and ~~, configured to allow access to the at least one audio content file only if the access is in compliance with the uses described in the at least one digital rights management license; and~~

wherein the media ~~at least one audio~~ content, ~~file,~~ the at least one digital rights management license, and the digital rights management software were installed on the computing device from a single ~~digital audio~~ storage medium that contained the content, the license, and the software.

40. (Currently Amended) The system of claim 39, further comprising:

a first identifier associated with the at least one digital rights management license;

a hard drive, coupled to the computing device;

a second ~~n~~-identifier, stored on the hard drive; and

wherein ~~the at least one digital rights management license is associated with a hard drive identifier so that~~ the digital rights management software, when executed by the computing device, causes the computing device to compare the first identifier to the second identifier before allowing a requested use of the media content. ~~does not allow access to the at least one audio content file unless the identifier with which the at least one license is associated is the same as the identifier stored on the hard drive.~~

41. (Original) The system of claim 39, wherein the digital rights management software comprises a generic module and a unique module.

42. (Currently Amended) The system of claim 39, further comprising:

at least one validation code ~~,~~ corresponding to at least one predetermined software module; and ~~computed prior to the software module being stored on the computing device; and~~

validation software that, when executed by the computing device, causes the computing device to compute at least one checksum for the at least one software module and compare the at least one checksum against the validation code ~~, configured~~ to determine if the at least one predetermined software module ~~s~~ should be ~~is~~ trusted. ~~by computing at least one checksum for at least one software module in the system and comparing those checksums against the prior computed validation code.~~

43. (Currently Amended) The system of claim 42, wherein:

the at least one validation code is a cryptographically-signed hash of a canonically-ordered series of bytes from the at least one predetermined software module; and

comparing the at least one checksum ~~s~~ against the ~~prior-computed~~ validation code comprises:

decrypting the cryptographically-signed hash;

performing a hash on the at least one software module ~~in the system~~; and

comparing the results of the two hashes to see if they match.

44. (Currently Amended) The system of claim 39, wherein the storage ~~audio~~ medium is a compact disc.

45. (Currently Amended) A method of transferring digital ~~audio~~ data from a removable ~~protected audio~~ storage medium to a storage device coupled to ~~on~~ a computing device, the method comprising:

copying the digital data ~~at least one encrypted audio file~~ from the removable ~~protected audio~~ storage medium to the storage device; ~~, along with encryption keys that can be used to decrypt these files; and~~

copying at least one digital rights management license from the removable ~~protected audio~~ storage medium to the storage device, the digital rights management license describing types of access that are allowed for the digital data; ~~at least one copied audio file;~~

copying digital rights management software from the removable storage medium to the storage device, wherein the ~~copied~~ digital rights management software, when executed by the computing device, causes the computing device to use ~~is configured to allow access to the at least one copied audio file only if the access is in compliance with the types of access described in~~ the at least one digital rights management license to determine whether or not an access to the digital data is permitted.

46. (Currently Amended) The method of claim 45, further comprising:

determining whether or not the computing device has ~~digital rights management software and~~ secure playback software that can read ~~are compatible with playing~~ the digital data; and ~~at least one encrypted audio file; and~~

installing ~~the compatible digital rights management software or~~ secure playback software if the computing device does not have the software. ~~them.~~

47. (Currently Amended) The method of claim 45, ~~46,~~ further comprising encrypting the at least one digital rights management license, and wherein the copied digital rights management software, when executed by the computing device, causes the computing device to deny ~~does not allow~~ access to the digital data on the storage device ~~at least one copied audio file~~ unless the at least one digital rights license is decrypted.

48. (Currently Amended) The method of claim 47, wherein encrypting the at least one digital rights management license comprises:

generating a binding identifier for the storage device;

storing the identifier on the storage device; ~~such that it is difficult to modify;~~

generating an encryption key from ~~using~~ the binding identifier; ~~as a key;~~ ~~and~~

encrypting the at least one digital rights management license using the generated encryption key; and

~~and~~ wherein the digital rights management software, when executed by the computing device, causes the computing device to use ~~is configured to create a decryption key for the at least one license using~~ the binding identifier to create a decryption key for the at least one license. ~~as a key.~~

49. (Currently Amended) The method of claim 45, wherein the removable storage ~~protected audio~~ medium is a compact disc.

50. (Currently Amended) A method of playing media content ~~digital data~~ stored on a removable storage ~~protected digital audio~~ medium ~~using digital rights management software on a computing device,~~ the method comprising:

reading digital data stored in a second format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a first format that also represents all or substantially all of the media content;

determining from ~~if the~~ at least one digital rights management license whether or not ~~on the digital audio medium allows~~ playback of the digital ~~audio~~ data stored in the second format is allowed. ~~thereon;~~

~~decrypting encrypted digital audio data contained on the protected digital audio medium in response to said determining; and~~

~~causing the decrypted digital audio data to be played on the computing device.~~

51. (Currently Amended) The method of claim 50, wherein the removable storage ~~protected digital audio~~ medium is a compact disc.

52. (Currently Amended) The method of claim 50, further comprising authenticating digital rights management software that, when executed by a computer, causes the computer to use the at least one digital rights management license to determine whether or not to allow playback of the digital data. ~~stored on the computing device to verify that it has not been tampered with or modified.~~

53. (Currently Amended) The method of claim 78, ~~52,~~ wherein the encrypted data ~~digital audio contained on the digital audio medium~~ comprises a plurality of encrypted packets of ~~audio~~ data.

54. (Currently Amended) The method of claim 53 wherein decrypting the data ~~digital audio contained on the digital audio medium~~ comprises:

locating at least one ~~audio~~ decryption key on the removable storage ~~digital audio~~ medium; and

using the at least one decryption key to decrypt ~~ing~~ the packets of ~~audio~~ data. ~~using at least one audio decryption key.~~

55. (Currently Amended) The method of claim 54, wherein:

~~each of~~ the at least one ~~audio~~ decryption key ~~s~~ is itself encrypted with a protection encryption key; and

the removable storage ~~digital audio~~ medium contains at least one protection decryption key to ~~which~~ decrypt ~~s~~ the at least one encrypted ~~audio~~ decryption key. ~~; and~~

~~wherein locating the at least one decryption key on the digital audio medium comprises decrypting the at least one encrypted audio decryption key using the at least one protection decryption key.~~

56. (Currently Amended) The method of claim 55, wherein:

the ~~at least one~~ protection encryption key ~~s~~ comprises a generic protection encryption key and a unique protection encryption key; and

the at least one protection decryption key ~~s~~ comprises a generic protection decryption ~~encryption~~ key and a unique protection decryption ~~encryption~~ key.

57. (Currently Amended) The method of claim 55, wherein the at least one ~~audio~~ decryption key is ~~s are~~ symmetric.

58. (Currently Amended) The method of claim 55, further comprising:

generating a symmetric playback protection key;

encrypting the at least one ~~audio~~ decryption key with the symmetric key; and

wherein decrypting the encrypted packets of digital data stored in the second format ~~audio~~ further comprises decrypting the at least one encrypted ~~audio~~ decryption key prior to decrypting the packets of ~~audio~~ data.

59. (Currently Amended) The method of claim 58, further comprises: ~~wherein~~

playing the encrypted digital data stored in the second format; and ~~audio further comprises~~

deleting the at least one ~~audio~~ decryption key and the decrypted packets of ~~audio~~ data from memory.

60. (Currently Amended) A method of transferring digital ~~audio~~ data stored on ~~from~~ a removable ~~protected digital audio~~ storage medium ~~a~~ to an external device, the method comprising:

loading digital rights management software from the ~~protected~~ medium; ~~a;~~

retrieving a digital rights management license from the ~~protected~~ medium; and ~~a;~~

using the digital rights management license to determine ~~ing~~ whether or not ~~that~~ a transfer of the digital ~~audio~~ data to the external device is allowed. ~~by the retrieved digital rights management license; and~~

~~transferring at least one audio file to the external device.~~

61. (Currently Amended) The method of claim 60, wherein the removable storage ~~protected~~ medium ~~a~~ is a compact disc.

62. (Currently Amended) The method of claim 60, further comprising authenticating the digital rights management software.

63. (Original) The method of claim 60, wherein the external device is a compact disc burner.

64. (Original) The method of claim 60, wherein the external device is a portable audio player.

65. (Currently Amended) The method of claim 79, ~~60,~~ further comprising translating the at least a portion of the digital data ~~one audio file~~ into a format that the ~~compatible with~~ the external device can read.

66. (Currently Amended) The method of claim 64, further comprising transferring the digital rights management software and the ~~at least one~~ digital rights management license from the removable storage ~~protected audio~~ medium ~~a~~ to the portable audio player. ~~external device.~~

67. (Currently Amended) The method of claim 66, wherein:

the portable audio player ~~external device~~ contains digital rights management software that is different than the software loaded from the removable storage medium; and

the method further comprises:

translating the ~~at least one~~ digital rights management license into a format that ~~compatible with~~ the software already on the portable audio player can read; and ~~external device; and~~

transferring the translated digital rights management license to the portable audio player. ~~external device.~~

68. (Currently Amended) A removable computer-readable storage medium storing media content and a program that, ~~readable by a computing device, the medium containing instructions which,~~ when executed by a computer, causes the computer to: ~~perform the method comprising:~~

read digital data stored on the medium in a second format and representing all or substantially all of the media content, wherein the medium also contains digital data stored in a first format that also represents all or substantially all of the media content;

locate ~~ing~~ a digital rights management license stored on the medium; and

using the digital rights management license to determine ~~ing~~ whether or not a requested use ~~if the license on the medium allows playback~~ of the digital data stored in the second format is allowed. ~~;~~

~~decrypting encrypted digital audio data contained on the medium; and~~

~~playing the decrypted audio data.~~

69. (Original) The medium of claim 68, wherein the medium is a compact disc.

70. (Currently Amended) The medium of claim 68, wherein the stored program further causes the computer to ~~comprising instructions which, when executed, perform the step of~~ authenticate ~~ing~~ the program. ~~software stored on the computing device to verify that it has not been tampered with or modified.~~

71. (Currently Amended) The medium of claim 80, ~~70,~~ wherein the encrypted ~~audio~~ data comprises encrypted packets of ~~audio~~ data.

72. (Currently Amended) The medium of claim 71, wherein the stored program further causes the computer to: ~~decrypting the audio data comprises:~~

locate ~~ing~~ a decryption key on the medium; and

decrypt ~~ing~~ the packets of ~~audio~~ data using the ~~audio~~ decryption key.

73. (Currently Amended) The medium of claim 72, wherein:

the decryption key is itself encrypted with a protection encryption key; and

the stored program further causes the computer to use the ~~medium contains a~~ protection decryption key to ~~which~~ decrypt ~~s~~ the encrypted ~~audio~~ decryption key; and

~~wherein locating the decryption key on the medium comprises decrypting the encrypted audio decryption key using the protection decryption key.~~

74. (Currently Amended) The medium of claim 73, wherein:

the protection encryption ~~decryption~~ key ~~s~~ comprises a generic protection encryption key and a unique protection encryption key; and

the protection decryption key ~~s~~ comprises a generic protection decryption ~~encryption~~ key and a unique protection decryption ~~encryption~~ key.

75. (Currently Amended) The medium of claim 73, wherein the ~~audio~~ decryption key is ~~s are~~ symmetric.

76. (Currently Amended) The medium of claim 73, wherein the stored program further causes the computer to: ~~further comprising instructions which, when executed, perform the steps of:~~

generate ~~ing~~ a symmetric playback protection key;

encrypt ~~ing~~ the ~~audio~~ decryption key with the symmetric key; and

~~wherein decrypting encrypted audio further comprises~~ decrypt ~~ing~~ the encrypted ~~audio~~ decryption key prior to decrypting the packets of ~~audio~~ data.

77. (Currently Amended) The medium of claim 76, wherein the stored program further causes the computer to:

play ~~ing~~ the encrypted digital data stored in the first format, and ~~audio further comprises~~

delete ~~ing~~ the ~~audio~~ decryption key and the decrypted packets of ~~audio~~ data from memory.

78. (New) The method of claim 50 wherein:

the digital data stored in the first format is encrypted, and

the method further comprises decrypting the encrypted data.

79. (New) The method of claim 60 further comprising transferring at least a portion of the digital data to the external device in response to the determination that the digital rights management license permits the transfer.

80. (New) The medium of claim 68, wherein:

The digital data stored in the second format is encrypted, and

the stored program further causes the computer to decrypt the encrypted data.

81. (New) A method of playing media content stored on a removable storage medium the method comprising:

reading digital data stored in a first format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a second format that also represents all or substantially all of the media content;

preventing an audio player configured to read the digital data stored in the second format from reading the digital data in the first format.

82. (New) The method of claim 81 wherein the first format comports to the Redbook compact disc standard.